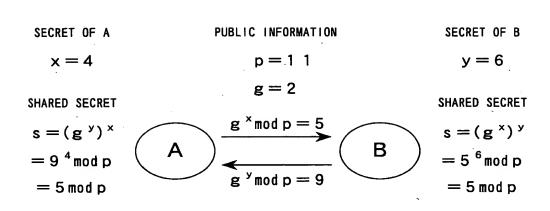


FIG. 1



F I G. 2

<u>i</u> = 4

p=2, $f(x)=x^3+x+1$

SECRET OF B
$$j = 6$$

$$g = x \mod f(x)$$

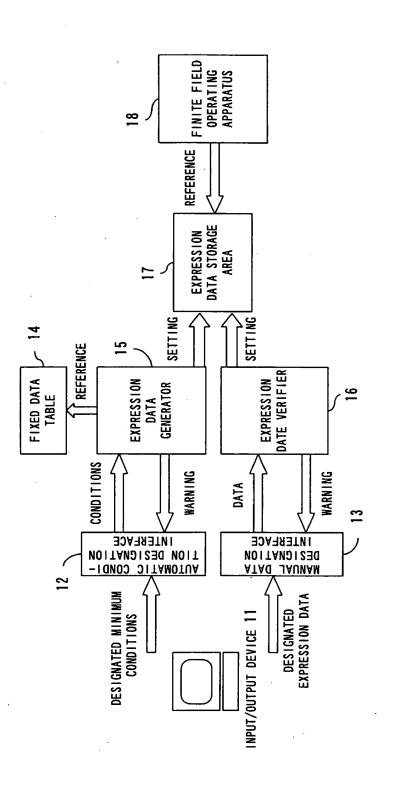
SHARED SECRET

$$g \mod f(x) = x^2 + x$$
 $g \mod f(x) = x^2 + x$
 $g \mod f(x) = x^2 + 1$
 $g \mod f(x) = x^2 + 1$
 $g \mod f(x) = x^2 + 1$

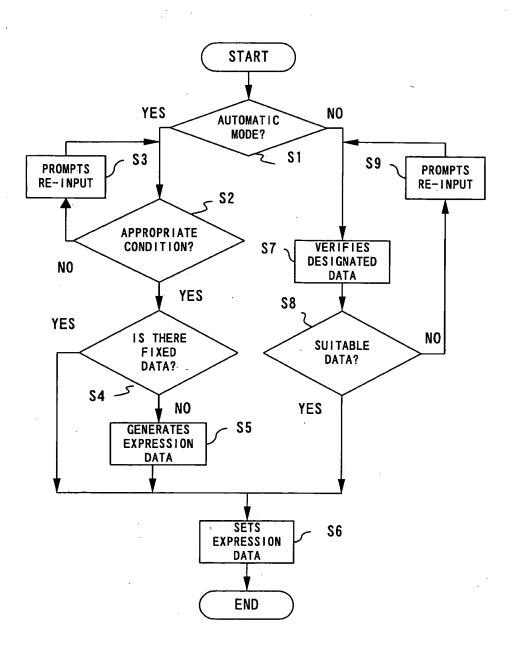
 $= (x^2+1)^4 \mod f(x)$

= x + 1

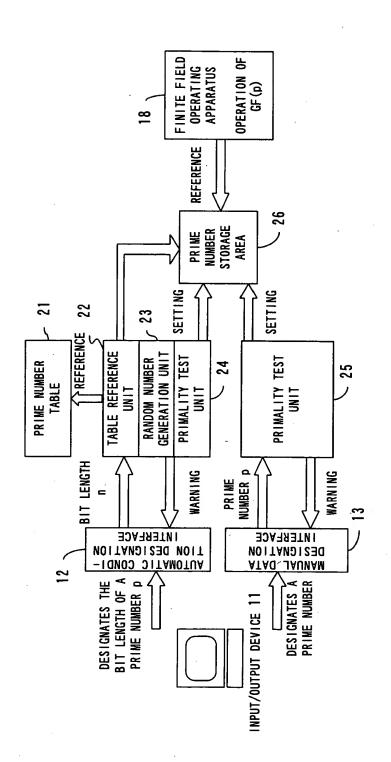
s = (g ^j) ⁱ



F I G. 4



F | G. 5



F I G. 6

BIT LENGTH n	PRIME NUMBER OF n BITS
2	3
3	7
4	11
:	:

F I G. 7

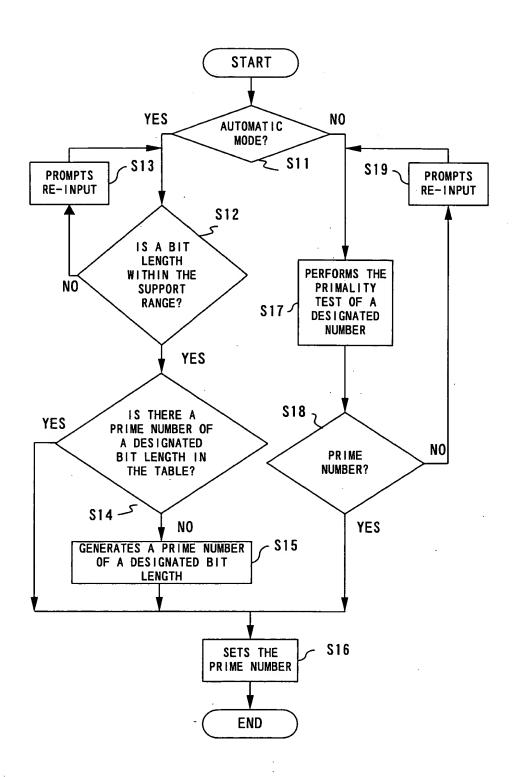
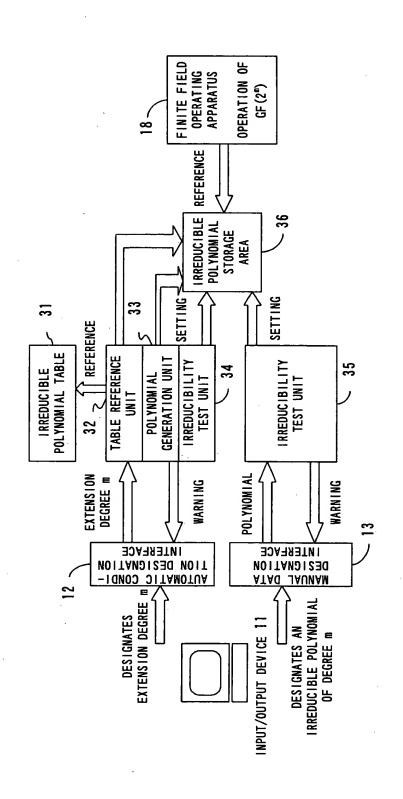


FIG. 8



F I G. 9

EXTENSION DEGREE	IRREDUCIBLE POLYNOMIAL OF DEGREE m
2	x ² +x+1
3	x ³ +x+1
4	x ⁴ +x+1
:	i i

FIG. 10

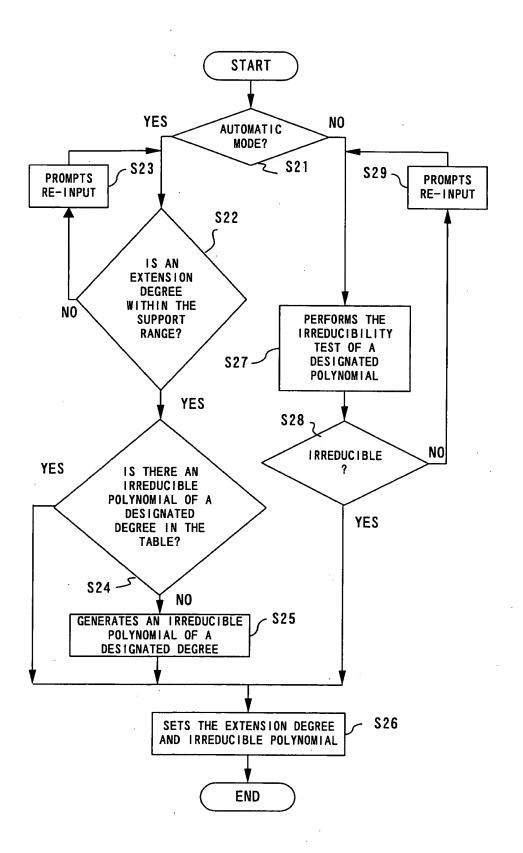


FIG. 11

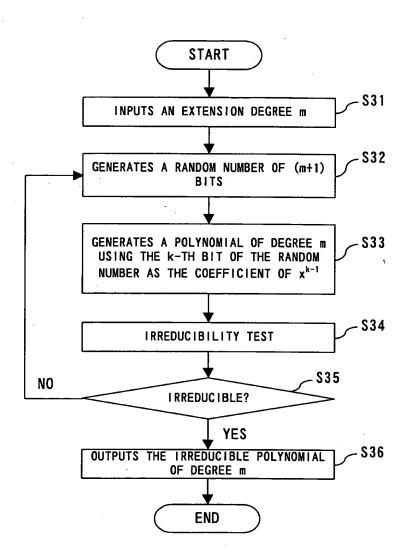


FIG. 12

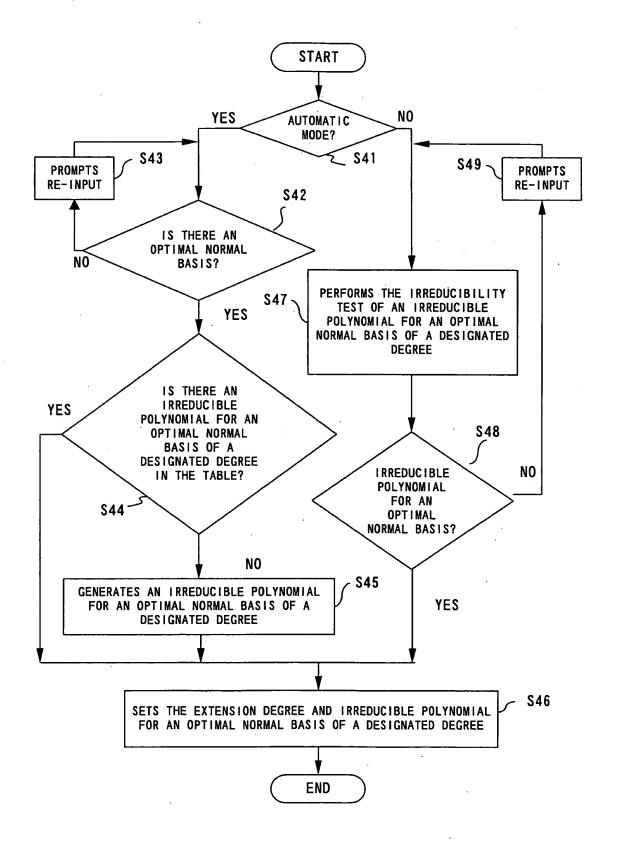


FIG. 13

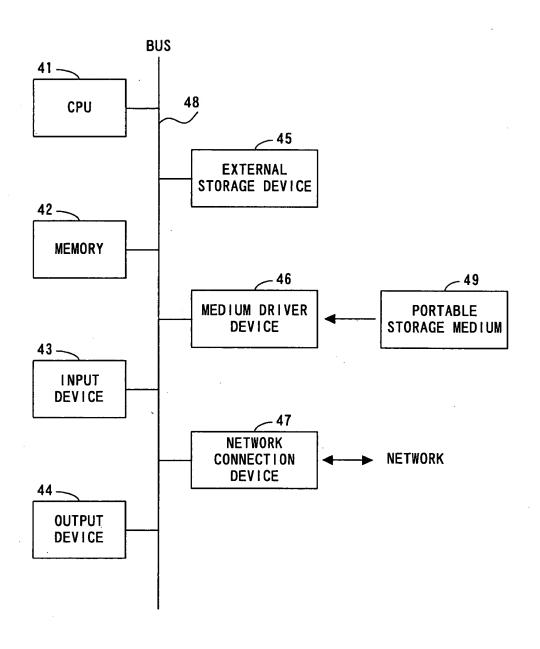
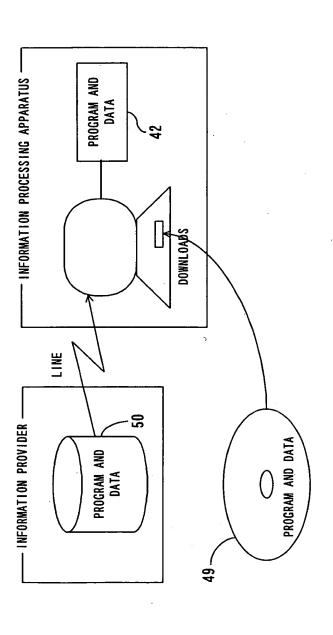


FIG. 14



F G. 15